Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

Claim 1 (currently amended): A computer-implemented method for use in a network environment including an enterprise server, comprising:

storing at the enterprise server multiple security credentials for a remote user to access respective secure resources residing on a network employing a generic application layer network protocol;

maintaining a map between a plurality of ~~one or more~~ resource servers and a type of security credential required to access each resource server, including maintaining a true/false flag and storing a path/domain for each of the plurality of resource servers;

receiving at the enterprise server a signal representing a request from the remote user for a first of the secure resources, wherein the request includes a logon credential for the remote user;

determining, by referring to the map and without the intervention of the user, that the type of security credential for the remote user that is required to access the first secure resource comprises a first of the security credentials corresponding to a first path/domain for a first of the resource servers for which the map indicates a true flag, and wherein the determining includes matching the first path/domain with a stored path/domain corresponding to said first of the resource servers;

sending from the enterprise server a signal representing a second request to retrieve the first secure resource, the second request including a first of the security credentials for the user of the type required to access the first secure resource;

receiving at the enterprise server a signal representing a first single-sign-on (SSO) credential generated by a first SSO provider based on the logon credential;

sending from the enterprise server a signal representing the first SSO credential to retrieve the first secure resource when the type of credential required to access the first secure resource includes the first SSO credential; and

sending from the enterprise server a signal representing the first SSO credential to retrieve the first secure resource when the type of credential required to access the first secure resource includes a second SSO credential corresponding to a second SSO provider having a trust relationship with the first SSO provider.

Claim 2 (original): The method of claim 1, further comprising:

authenticating the user before sending the signal representing the second request.

Claim 3 (previously presented): The method of claim 1, further comprising:

receiving at the enterprise server a signal representing a response to the second request; and

sending from the enterprise server a signal representing a result to the remote user, the result based on the response to the second request.

Claim 4 (previously presented): The method of claim 1, wherein the request includes a logon credential for the remote user, the method further comprising: authenticating the remote user based on the logon credential before sending the second request.

Claim 5 (previously presented): The method of claim 1, wherein the request includes a logon credential for the remote user and the type of security credential

required to access the first secure resource includes the logon credential, the method further comprising:

sending the signal representing the second request to retrieve the first secure resource, the second request including the logon credential.

Claim 6 (canceled)

Claim 7 (canceled)

Claim 8 (currently amended): A computer-implemented method for use in a network environment including an enterprise server, comprising:

storing at the enterprise server multiple security credentials for a remote user to access respective secure resources residing on a network employing a generic application layer network protocol;

maintaining a map between a plurality of ~~one or more~~ resource servers and a type of security credential required to access each resource server, including maintaining a true/false flag and storing a path/domain for each of the plurality of resource servers;

receiving at the enterprise server a signal representing a request from the remote user for a first of the secure resources, wherein the request includes a logon credential for the remote user;

determining, by referring to the map and without the intervention of the user, that the type of security credential for the remote user that is required to access the first secure resource comprises a first of the security credentials corresponding to a first path/domain for a first of the resource servers for which the map indicates a true flag, and wherein the determining includes matching the first path/domain with a stored path/domain corresponding to said first of the resource servers;

sending from the enterprise server a signal representing a second request to retrieve the first secure resource, the second request including a first of the security credentials for the user of the type required to access the first secure resource;

receiving at the enterprise server a signal representing a first single-sign-on (SSO) credential generated by a first SSO provider based on the logon credential;

sending from the enterprise server a signal representing the first SSO credential to retrieve the first secure resource when the type of credential required to access the first secure resource includes the first SSO credential;

receiving at the enterprise server a signal representing a second SSO credential generated by a second SSO provider based on the first SSO credential; and

sending from the enterprise server a signal representing the second SSO credential to retrieve the first secure resource when the type of credential required to access the first secure resource includes the second SSO credential.

Claim 9 (original): The method of claim 1, wherein the generic application-layer network protocol is hypertext transfer protocol.

Claim 10 (previously presented): The method of claim 9, further comprising:

receiving at the enterprise server a signal representing data in response to the second request; and

sending from the enterprise server a signal representing at least a portion of the data to the remote user.

Claim 11 (previously presented): The method of claim 10, wherein the first secure resource includes a Web site, and the data is hypertext mark-up language.

Claim 12 (currently amended): A computer-implemented method for use in a network environment including an enterprise server, comprising:

storing at the enterprise server multiple security credentials for a remote user to access respective secure resources residing on a network employing a generic application layer network protocol;

maintaining a map between a plurality of ~~one or more~~ resource servers and a type of security credential required to access each resource server, including maintaining a true/false flag and storing a path/domain for each of the plurality of resource servers;

receiving at the enterprise server a signal representing a request from the remote user for a first of the secure resources, wherein the request includes a logon credential for the remote user;

determining, by referring to the map and without the intervention of the user, that the type of security credential for the remote user that is required to access the first secure resource comprises a first of the security credentials corresponding to a first path/domain for a first of the resource servers for which the map indicates a true flag, and wherein the determining includes matching the first path/domain with a stored path/domain corresponding to said first of the resource servers;

sending from the enterprise server a signal representing a second request to retrieve the first secure resource, the second request including a first of the security credentials for the user of the type required to access the first secure resource, wherein the receiving includes receiving at the enterprise server a signal representing a third request from the remote user for a second of the secure resources residing on the network,

determining, without the intervention of the user, the type of security credential for the remote user that is required to access the second secure resource; and

sending from the enterprise server a signal representing a fourth request for retrieving the second secure resource, the fourth request including a second of the security credentials for the user of the type required to access the second secure resource; and wherein the signals representing the second and fourth requests are sent concurrently.

Claim 13 (previously presented): The method of claim 12, wherein the types of security credentials included in the second and fourth requests differ.

Claim 14 (previously presented): The method of claim 12, wherein the types of security credentials included in the second and fourth requests are the same.

Claim 15 (canceled)

Claim 16 (canceled)

Claim 17 (currently amended): An apparatus for use in a network environment including an enterprise server, comprising:

means for storing at the enterprise server multiple security credentials for a remote user to access respective secure resources residing on a network employing a generic application layer network protocol;

means for maintaining a map between a plurality of ~~one or more~~ resource servers and a type of security credential required to access each resource server, including maintaining a true/false flag and storing a path/domain for each of the plurality of resource servers;

means for receiving at the enterprise server a signal representing a request from the remote user for a first of the secure resources;

means for determining, by referring to the map and without the intervention of the user, that the type of security credential for the remote user

that is required to access the first secure resource comprises a first of the security credentials corresponding to a first path/domain for a first of the resource servers for which the map indicates a true flag, and wherein the determining includes matching the first path/domain with a stored path/domain corresponding to said first of the resource servers;

means for sending from the enterprise server a signal representing a second request to retrieve the first secure resource, the second request including a first of the security credentials for the user of the type required to access the first secure resource, wherein the request includes a logon credential for the remote user;

means for receiving at the enterprise server a signal representing a first single-sign-on (SSO) credential generated by a first SSO provider based on the logon credential;

means for sending from the enterprise server a signal representing the first SSO credential to retrieve the first secure resource when the type of credential required to access the first secure resource includes the first SSO credential; and

means for sending from the enterprise server a signal representing the first SSO credential to retrieve the first secure resource when the type of credential required to access the first secure resource includes a second SSO credential corresponding to a second SSO provider having a trust relationship with a first SSO provider.

Claim 18 (original): The apparatus of claim 17, further comprising:

means for authenticating the user before sending the signal representing the second request.

Claim 19 (previously presented): The apparatus of claim 17, further comprising:

means for receiving at the enterprise server a signal representing a response to the second request; and

means for sending from the enterprise server a signal representing a result to the remote user, the result based on the response to the second request.

Claim 20 (previously presented): The apparatus of claim 17, wherein the request includes a logon credential for the remote user, the apparatus further comprising:

means for authenticating the remote user based on the logon credential before sending the second request.

Claim 21 (previously presented): The apparatus of claim 17, wherein the request includes a logon credential for the remote user and the type of security credential required to access the first secure resource includes the logon credential, the apparatus further comprising:

means for sending from the enterprise server the signal representing the second request to retrieve the first secure resource, the second request including the logon credential.

Claim 22 (canceled)

Claim 23 (canceled)

Claim 24 (currently amended): An apparatus for use in a network environment including an enterprise server, comprising:

means for storing at the enterprise server multiple security credentials for a remote user to access respective secure resources residing on a network employing a generic application layer network protocol;

means for maintaining a map between a plurality of ~~one or more~~ resource servers and a type of security credential required to access each resource server, including maintaining a true/false flag and storing a path/domain for each of the plurality of resource servers;

means for receiving at the enterprise server a signal representing a request from the remote user for a first of the secure resources;

means for determining, by referring to the map and without the intervention of the user, that the type of security credential for the remote user that is required to access the first secure resource comprises a first of the security credentials corresponding to a first path/domain for a first of the resource servers for which the map indicates a true flag, and wherein the determining includes matching the first path/domain with a stored path/domain corresponding to said first of the resource servers;

means for receiving at the enterprise server a signal representing a first single-sign-on (SSO) credential generated by a first SSO provider based on the logon credential;

means for sending from the enterprise server a signal representing the first SSO credential to retrieve the first secure resource when the type of credential required to access the first secure resource includes the first SSO credential;

means for sending from the enterprise server a signal representing a second request to retrieve the first secure resource, the second request including a first of the security credentials for the user of the type required to access the first secure resource, wherein the request includes a logon credential for the remote user;

means for receiving at the enterprise server a signal representing a second SSO credential generated by a second SSO provider based on a ~~the~~ first SSO credential; and

means for sending from the enterprise server a signal representing the second SSO credential to the secure resource when the type of credential required to access the secure resource includes the second SSO credential.

Claim 25 (original): The apparatus of claim 17, wherein the generic application-layer network protocol is hypertext transfer protocol.

Claim 26 (previously presented): The apparatus of claim 25, further comprising:

means for receiving at the enterprise server a signal representing data in response to the second request; and

means for sending from the enterprise server a signal representing at least a portion of the data to the remote user.

Claim 27 (previously presented): The apparatus of claim 26, wherein the first secure resource includes a Web site, and the data is hypertext mark-up language.

Claim 28 (previously presented): The apparatus of claim 17, wherein the means for receiving includes means for receiving at the enterprise server a signal representing a third request from the remote user for a second secure resource residing on the network, the apparatus further comprising:

means for determining, without the intervention of the user, the type of security credential for the remote user that is required to access the second secure resource; and

means for sending from the enterprise server a signal representing a fourth request to retrieve the second secure resource, the fourth request including a second of the security credentials for the user of the type required to access the second secure resource; and

wherein the signals representing the second and fourth requests are sent concurrently.

Claim 29 (previously presented): The apparatus of claim 28, wherein the types of security credentials included in the second and fourth requests differ.

Claim 30 (previously presented): The apparatus of claim 28, wherein the types of security credentials included in the second and fourth requests are the same.

Claim 31 (previously presented): The apparatus of claim 17, further comprising:

means for receiving at the enterprise server a signal representing the first security credential from the user before receiving the signal representing the first request.

Claim 32 (canceled)

Claim 33 (currently amended): One or more computer-readable media tangibly embodying a program of instructions executable by a computer to perform a method for use in a network environment including an enterprise server, the method comprising:

storing at the enterprise server multiple security credentials for a remote user to access respective secure resources residing on a network employing a generic application layer network protocol;

maintaining a map between a plurality of ~~one or more~~ resource servers and a type of security credential required to access each resource server, including maintaining a true/false flag and storing a path/domain for each of the plurality of resource servers;

receiving at the enterprise server a signal representing a request from the remote user for a first of the secure resources, wherein the request includes a logon credential for the remote user;

determining, by referring to the map and without the intervention of the user, that the type of security credential for the remote user that is required to access the first secure resource comprises a first of the security credentials corresponding to a first path/domain for a first of the resource servers for which the map indicates a true flag, and wherein the determining includes matching the first path/domain with a stored path/domain corresponding to said first of the resource servers;

sending from the enterprise server a signal representing a second request to retrieve the first secure resource, the second request including a first of the security credentials for the user of the type required to access the first secure resource;

receiving at the enterprise server a signal representing a first single-sign-on (SSO) credential generated by a first SSO provider based on the logon credential;

sending from the enterprise server a signal representing the first SSO credential to retrieve the first secure resource when the type of credential required to access the first secure resource includes the first SSO credential; and

sending from the enterprise server a signal representing the first SSO credential to retrieve the first secure resource when the type of credential required to access the first secure resource includes a second SSO credential corresponding to a second SSO provider having a trust relationship with a first SSO provider.

Claim 34 (original): The media of claim 33, wherein the method further comprises:

authenticating the user before sending the signal representing the second request.

Claim 35 (previously presented): The media of claim 33, wherein the method further comprises:

receiving at the enterprise server a signal representing a response to the second request; and

sending from the enterprise server a signal representing a result to the remote user, the result based on the response to the second request.

Claim 36 (original): The media of claim 33, wherein the request includes a logon credential for the remote user, wherein the method further comprises:

authenticating the remote user based on the logon credential before sending the second request.

Claim 37 (previously presented): The media of claim 33, wherein the request includes a logon credential for the remote user and the type of security credential required to access the first secure resource includes the logon credential, wherein the method further comprises:

sending from the enterprise server the signal representing the second request to retrieve the first secure resource, the second request including the logon credential.

Claim 38 (canceled)

Claim 39 (canceled)

Claim 40 (currently amended): One or more computer-readable media tangibly embodying a program of instructions executable by a computer to perform a

method for use in a network environment including an enterprise server, the method comprising:

storing at the enterprise server multiple security credentials for a remote user to access respective secure resources residing on a network employing a generic application layer network protocol;

maintaining a map between a plurality of ~~one or more~~ resource servers and a type of security credential required to access each resource server, including maintaining a true/false flag and storing a path/domain for each of the plurality of resource servers;

receiving at the enterprise server a signal representing a request from the remote user for a first of the secure resources, wherein the request includes a logon credential for the remote user;

determining, by referring to the map and without the intervention of the user, that the type of security credential for the remote user that is required to access the first secure resource comprises a first of the security credentials corresponding to a first path/domain for a first of the resource servers for which the map indicates a true flag, and wherein the determining includes matching the first path/domain with a stored path/domain corresponding to said first of the resource servers;

sending from the enterprise server a signal representing a second request to retrieve the first secure resource, the second request including a first of the security credentials for the user of the type required to access the first secure resource;

receiving at the enterprise server a signal representing a first single-sign-on (SSO) credential generated by a SSO provider based on the logon credential;

sending from the enterprise server a signal representing the first SSO credential to retrieve the first secure resource when the type of credential required to access the first secure resource includes the first SSO credential;

receiving at the enterprise server a signal representing a second SSO credential generated by a second SSO provider based on the first SSO credential; and

sending from the enterprise server a signal representing the second SSO credential to retrieve the first secure resource when the type of credential required to access the first secure resource includes the second SSO credential.

Claim 41 (original): The media of claim 33, wherein the generic application-layer network protocol is hypertext transfer protocol.

Claim 42 (previously presented): The media of claim 41, wherein the method further comprises:

receiving at the enterprise server a signal representing data in response to the second request; and

sending from the enterprise server a signal representing at least a portion of the data to the remote user.

Claim 43 (previously presented): The media of claim 42, wherein the first secure resource includes a Web site, and the data is hypertext mark-up language.

Claim 44 (currently amended): One or more computer-readable media tangibly embodying a program of instructions executable by a computer to perform a method for use in a network environment including an enterprise server, the method comprising:

storing at the enterprise server multiple security credentials for a remote user to access respective secure resources residing on a network employing a generic application layer network protocol;

maintaining a map between a plurality of ~~one or more~~ resource servers and a type of security credential required to access each resource server;

including maintaining a true/false flag and storing a path/domain for each of the plurality of resource servers;

receiving at the enterprise server a signal representing a request from the remote user for a first of the secure resources, wherein the request includes a logon credential for the remote user;

determining, by referring to the map and without the intervention of the user, that the type of security credential for the remote user that is required to access the first secure resource comprises a first of the security credentials corresponding to a first path/domain for a first of the resource servers for which the map indicates a true flag, and wherein the determining includes matching the first path/domain with a stored path/domain corresponding to said first of the resource servers;

sending from the enterprise server a signal representing a second request to retrieve the first secure resource, the second request including a first of the security credentials for the user of the type required to access the first secure resource, wherein the receiving includes receiving at the enterprise server a signal representing a third request from the remote user for a second secure resource residing on the network,

determining, without the intervention of the user, the type of security credential for the remote user that is required to access the second secure resource; and

sending from the enterprise server a signal representing a fourth request for retrieving the second secure resource, the fourth request including a second security credential for the user of the type required to access the second secure resource; and

wherein the signals representing the second and fourth requests are sent concurrently.

Claim 45 (previously presented): The media of claim 44, wherein the types of security credentials included in the second and fourth requests differ.

Claim 46 (previously presented): The media of claim 44, wherein the types of security credentials included in the second and fourth requests are the same.

Claim 47 (canceled)

Claim 48 (canceled)

Claim 49 (previously presented): The method of claim 8, further comprising:

authenticating the user before sending the signal representing the second request.

Claim 50 (previously presented): The method of claim 8, further comprising:

receiving at the enterprise server a signal representing a response to the second request; and

sending from the enterprise server a signal representing a result to the remote user, the result based on the response to the second request.

Claim 51 (previously presented): The method of claim 8, wherein the request includes a logon credential for the remote user, the method further comprising: authenticating the remote user based on the logon credential before sending the second request.

Claim 52 (previously presented): The method of claim 8, wherein the request includes a logon credential for the remote user and the type of security credential required to access the first secure resource includes the logon credential, the method further comprising:

sending the signal representing the second request to retrieve the first secure resource, the second request including the logon credential.

Claim 53 (previously presented): The method of claim 8, wherein the generic application-layer network protocol is hypertext transfer protocol.

Claim 54 (previously presented): The method of claim 53, further comprising:

receiving at the enterprise server a signal representing data in response to the second request; and

sending from the enterprise server a signal representing at least a portion of the data to the remote user.

Claim 55 (previously presented): The method of claim 54, wherein the first secure resource includes a Web site, and the data is hypertext mark-up language.

Claim 56 (previously presented): The method of claim 12, wherein the generic application-layer network protocol is hypertext transfer protocol.

Claim 57 (previously presented): The method of claim 56, further comprising:

receiving at the enterprise server a signal representing data in response to the second request; and

sending from the enterprise server a signal representing at least a portion of the data to the remote user.

Claim 58 (previously presented): The method of claim 57, wherein the first secure resource includes a Web site, and the data is hypertext mark-up language.

Claim 59 (previously presented): The method of claim 17, wherein the generic application-layer network protocol is hypertext transfer protocol.

Claim 60 (previously presented): The method of claim 59, further comprising:

receiving at the enterprise server a signal representing data in response to the second request; and

sending from the enterprise server a signal representing at least a portion of the data to the remote user.

Claim 61 (previously presented): The method of claim 60, wherein the first secure resource includes a Web site, and the data is hypertext mark-up language.

Claim 62 (previously presented): The apparatus of claim 24, wherein the generic application-layer network protocol is hypertext transfer protocol.

Claim 63 (previously presented): The apparatus of claim 62, further comprising:

means for receiving at the enterprise server a signal representing data in response to the second request; and

means for sending from the enterprise server a signal representing at least a portion of the data to the remote user.

Claim 64 (previously presented): The apparatus of claim 63, wherein the first secure resource includes a Web site, and the data is hypertext mark-up language.

Claim 65 (previously presented): The apparatus of claim 24, wherein the means for receiving includes means for receiving at the enterprise server a signal

representing a third request from the remote user for a second secure resource residing on the network, the apparatus further comprising:

means for determining, without the intervention of the user, the type of security credential for the remote user that is required to access the second secure resource; and

means for sending from the enterprise server a signal representing a fourth request to retrieve the second secure resource, the fourth request including a second of the security credentials for the user of the type required to access the second secure resource; and

wherein the signals representing the second and fourth requests are sent concurrently.

Claim 66 (previously presented): The apparatus of claim 65, wherein the types of security credentials included in the second and fourth requests differ.

Claim 67 (previously presented): The apparatus of claim 65, wherein the types of security credentials included in the second and fourth requests are the same.

Claim 68 (previously presented): The apparatus of claim 24, further comprising:

means for receiving at the enterprise server a signal representing the first security credential from the user before receiving the signal representing the first request.

Claim 69 (previously presented): The media of claim 40, wherein the method further comprises:

authenticating the user before sending the signal representing the second request.

Claim 70 (previously presented): The media of claim 40, wherein the method further comprises:

receiving at the enterprise server a signal representing a response to the second request; and

sending from the enterprise server a signal representing a result to the remote user, the result based on the response to the second request.

Claim 71 (previously presented): The media of claim 40, wherein the request includes a logon credential for the remote user, wherein the method further comprises:

authenticating the remote user based on the logon credential before sending the second request.

Claim 72 (previously presented): The media of claim 40, wherein the request includes a logon credential for the remote user and the type of security credential required to access the first secure resource includes the logon credential, wherein the method further comprises:

sending from the enterprise server the signal representing the second request to retrieve the first secure resource, the second request including the logon credential.

Claim 73 (previously presented): The media of claim 40, wherein the generic application-layer network protocol is hypertext transfer protocol.

Claim 74 (previously presented): The media of claim 73, wherein the method further comprises:

receiving at the enterprise server a signal representing data in response to the second request; and

sending from the enterprise server a signal representing at least a portion of the data to the remote user.

Claim 75 (previously presented): The media of claim 74, wherein the first secure resource includes a Web site, and the data is hypertext mark-up language.

Claim 76 (previously presented): The media of claim 44, wherein the generic application-layer network protocol is hypertext transfer protocol.

Claim 77 (previously presented): The media of claim 76, wherein the method further comprises:

receiving at the enterprise server a signal representing data in response to the second request; and

sending from the enterprise server a signal representing at least a portion of the data to the remote user.

Claim 78 (previously presented): The media of claim 77, wherein the first secure resource includes a Web site, and the data is hypertext mark-up language.

Claims 79-84 (canceled)